REMARKS

Claims 1 – 124 are pending in the application. Claims 1, 69, 109, and 110 are currently amended.

1. Page 9, line 17 of the disclosure was objected to for including reference to the number "18". Page 9 has now been corrected.

2. The Examiner objected to the drawings for having handwritten numbers and crossed out labels. Applicant has reviewed the drawings filed on December 6, 2001 on the Public PAIR page and did not view any handwritten numbers or crossed out labels and thus did not make any corrections. Withdrawal of this objection is respectfully requested.

Claim Rejections – 35 USC 112

3. The Examiner rejected claims 1, 69, 109, and 110 under 35 USC 112, second paragraph, as being indefinite for failing to particularly point out and claim the matter which the applicant regards as the invention. More specifically, the Examiner argued that it is not clear what the prefix "pre" in the terms: "prestored" and "preobtained", in the rejected claims, refers to.

Claims 1, 69, 109, and 110 are amended so as to clearly define what the prefix "pre" refers to. Favorable reconsideration of this rejection in view of the above amendments is respectfully requested.

Claim Rejections – 35 USC 102

4. In this section of the official action, Claims 1-4, 11, 51, 56-65, 69, 70, 109, 110, 111, and 112 were rejected under 35 USC 102(e) as being anticipated by Kephart US Patent No. 6,732,149.

Favorable reconsideration of this rejection in view of the above amendments and the following explanations is respectfully requested.

The present application describes a system for network content monitoring and control. The system described by the present application relates to the monitoring of digital content transport, for enforcing copyright, secrecy, and confidentiality with respect to the transported digital content. The present application defines in the field of invention section: "The present invention relates to monitoring transport of digital content, particularly but not exclusively for the enforcement of digital copyright, secrecy, and confidentiality".

That is to say, the present invention aims at controlling the movement of known digital content regarded as confidential, secret, protected by copyright, etc. With the present invention, transported digital content is examined. If the examined digital content is identified as belonging to known sensitive content which is confidential, secret, protected by copyright, etc, the movement of the digital content identified as sensitive content may be limited according to a predefined policy with respect to the identified content.

Kephart US Patent No. 6,732,149 teaches a system and a method for protection against SPAM, as described in the field of invention section: "the present invention relates to a system and method for automatically detecting and handling unsolicited and undesired electronic mail such as Unsolicited Commercial E-mail (UCE), also referred to as "spam".

Kephart examines electronic mail for determining if the mail bears patterns of SPAM, and blocks such mail. However Kephart does not disclose or even hint at a method or at an apparatus where a transported message is examined for determining if the message comprises known confidential content, known secret content, known content protected by copyright, etc, as taught by the present invention.

Claim 1, as currently amended, defines a system for network content monitoring, comprising: a transport data monitor, connectable to a point in a network, for monitoring data being transported past the point, a description extractor, associated with the transport data monitor, for extracting descriptions of the data being transported, a database of at least one preobtained description of known content whose movements it is desired to monitor, the preobtained description being obtained in advance of the extracting descriptions, and a comparator, configured to determine whether the extracted description corresponds to any of the at least one preobtained descriptions, *and to decide whether the data being transported comprises any of the content whose movements it is desired to monitor according to the determining.*

As described hereinabove, Kephart falls short of teaching or even hinting at a system which comprises a comparator *for deciding whether data being transported comprises any of the known content whose movements it is desired to monitor.*

That is to say, Kephart teaches **categorization** of electronic messages (e-mail), aimed at deciding whether an electronic message (e-mail) should be categorized as SPAM, whereas the present invention teaches **identification** of transport data as belonging to a ***specific known*** content whose movements it is desired to monitor, as taught by the present invention and defined by claim 1

It is thus respectfully believed that claim 1 is both novel and inventive over the prior art, and maintained that claim 1 is allowable.

Claim 69, as amended, defines a system for network content control, comprising: a transport data monitor, connectable to a point in a network, for monitoring data being transported past the point, a signature extractor, associated with the transport data monitor, for extracting a derivation of payload of the monitored data, the derivation being indicative of content of the data, a database of preobtained signatures of known content whose movements it is desired to monitor, the preobtained signatures being obtained in advance of the extracting a derivation of payload, a comparator for comparing the derivation with the preobtained signatures, *and to determine whether the monitored data comprises any of the content whose movements it is desired to control*, a decision-making unit for producing an enforcement decision, using the output of the comparator, and a bandwidth management unit connected to the decision-making unit for managing network bandwidth assignment in accordance with output decisions of the policy determinator, thereby to control content distribution over the network.

As described hereinabove, Kephart falls short of teaching or even hinting at a system which comprises a comparator for *deciding whether the monitored data comprises any of the known content whose movements it is desired to monitor*. Furthermore, Kephart also falls short of teaching or even hinting at the idea of managing *network bandwidth assignment*, in accordance with a decision with regards to a monitored data's comprising of any of the known content whose movements it is desired to monitor, as taught by the present invention and defined by claim 69.

It is thus respectfully believed that claim 69 is both novel and inventive over the prior art, and maintained that claim 69 is allowable, as taught by the present invention and defined by claim 69.

Claim 109, as amended, defines a method of monitoring for distribution of known sensitive content over a network, the method comprising: obtaining extracts of data from at least one monitoring point on the network, obtaining a signature indicative of content of the extracted data, comparing the signature with at least one of a set of signatures indicative of the sensitive content, the set of signatures being stored in advance of the obtaining extracts of data, *determining if the extracted data comprises any of the sensitive content* according to the comparing, and using an output of the determining as an indication of the presence or absence of the sensitive content.

As described hereinabove, Kephart falls short of teaching or even hinting at a method which comprises *determining if the extracted data comprises known sensitive content*, as taught by the present invention and defined by claim 109.

It is thus respectfully believed that claim 109 is both novel and inventive over the prior art, and maintained that claim 109 is allowable.

Claim 110 as amended defines a method of controlling the distribution of known sensitive content over a network, the method comprising: obtaining extracts of data from at least one monitoring point on the network, obtaining a signature indicative of content of the extracted data, comparing the signature with at least one of a set of signatures indicative of the sensitive content, the set being stored in advance of the obtaining extracts of data, *determining if the extracted data comprises any of the sensitive content according to the comparing*, using an output of the determining in selecting an enforcement decision, and

using the enforcement decision in bandwidth management of the network.

As described hereinabove, Kephart falls short of teaching or even hinting at a method which comprises *determining if the extracted data comprises known sensitive content*, as taught by the present invention and defined by claim 110

It is thus respectfully believed that claim 110 is both novel and inventive over the prior art, and maintained that claim 110 is allowable.

All dependent claims are believed to be allowable as being dependent upon an allowable main claim.

All of the matters raised by the Examiner have been dealt with and are believed to have been overcome.

In view of the foregoing, it is respectfully submitted that all the claims now pending in the application are allowable over the cited reference. An early Notice of Allowance is therefore respectfully requested.

Respectfully submitted,
Martin D. Moynihan
Martin D. Moynihan
Registration No. 40,338

Date: May 22, 2006